SAR guidance consultation – Batch 21-30 – Response 26

Answer to question 2

Where you talk about requests made via social media on page 10, you state in the final paragraph of that section that in most cases it won't be appropriate to send the response to the SAR via social media and we should ask for an alternative delivery address for the response. It would be useful to include here what a controller's obligations are if the individual refuses to provide an alternative address, ignores the request or specifically instructs us to respond via social media. If they refuse to provide an alternative address and it is possible to send the response via social media, but is not secure, are we in breach of our obligations if we then do not send the SAR response via social media? Similarly, if they instruct us to send it via social media and we know it is not secure, are we in breach of our security obligations under the GDPR if we comply with the request? These come up often in large organisations and it would be helpful to have clarity on these points.

On the issue of deleted, archived or backed up data and SAR as set out on page 25, further clarity around back-up and deletion is required. It is fairly clear that archived data is still retained for active business purposes and should be provided in response to a SAR. The guidance you provide around deletion and backups in contradictory. Information is deleted for business purposes in the normal course of business and is inaccessible to any employee except those in the IT function with the ability to restore files or systems from backups. The data is deleted for business purposes but is also backed up. It is only backed up with the intention of restoring it in the event of an emergency; it will not be routinely accessed from backups for any business purposes other than restoring data to its original state in the event of a system fault or some kind of catastrophic event. We need clarification on whether this deleted yet backed up data is covered by the SAR provisions. If it is to be provided in response to a SAR, what is the point in ever deleting anything if it is never actually classed as deleted for GDPR purposes because it would have to be reconstituted following a SAR? Further clarity would be helpful to controllers. The issue particularly crops up in relation to emails. Where emails are deleted and inaccessible to all but a few technical staff, but could technically be accessed by restoring a user's mailbox back to a specific point in time, are these covered? They are deleted for our business purposes, almost always never to be looked at again (other than the scenarios set out above) but they are retrievable from backups for a certain period of time.

It would also be helpful to have further detail on the method of searches we are required to carry out. For example, when a large organsiation receives a request for emails sent by named members of staff, usual practice is that those members of staff are asked to provide any relevant emails to the DPO's team which will then consider and prep them for disclosure. Staff are made aware of the consequences of withholding or deleting emails to prevent disclosure. Is this acceptable? is this what the ICO does? Should the DPO's team be given access to 3000+ employee mailboxes to carry out the searches centrally? I would argue not, from a privacy and resource perspective. Also, if these should be done centrally, where is the line drawn? Should access be given to all of the network for central searches to be carried out? Is this a decision for individual controllers to take? The question is asked often by controllers is discussion forums so would be helpful to address. The guidance seems to focus on controllers having an information management system they can simply query to provide all the information; however in reality a large, complex organisation will have many different systems, as well as many different networked and physical locations which all contain personal data.

Finally, on the issue of asking for clarification (page 23 and 24): it is unclear how we're expected to proceed with requests where we ask for clarifcation or help to locate the data but aren't able to stop the clock while we wait for a response. Requests are regularly received for 'all personal data held' but when we ask them to provide info to help us locate the data, it is only a small subset of the information we actually hold that they are asking for. if the default position is that when a request for 'everything' is received, the clock starts and we need to start collating everything (which could be thousands of items of data) while we wait for them to reply to our query about whether they actually want everything, this is a massive waste of resource when they reply to say they only want a tiny proportion of what we actually hold. This seems to be a major shift from previous practice where it was acceptable to ask for further clarifcation to help locate the personal data and pause the clock.